IN THE SPECIFICATION

Please enter the following amendments to the description:

Please re-write paragraph [0012] to read as follows:

[0012] There is a so-called open key ciphering process which utilizes such an algorithm based on such a ciphering process with a ciphering key and such a decoding process with a decoding key being different algorithms from each other. The open key ciphering process utilizes such an open key commonly usable by unspecified users. This ciphering method ciphers a document addressed to a specific individual by applying an open key issued by this specific individual. The document ciphered by this open key can be decoded solely by applying a secrete key corresponding to this open key used for ciphering this document. Inasmuch as the secrete key is reserved by such a specific individual who issued the open key, the document ciphered by the open key can exclusively be decoded by a specific individual reserving the secrete key. The RSA (Rivest Shamir Adleman) ciphering code is cited as the typical system of the open key ciphering method cited above. By way of utilizing the open key ciphering method, it is possible to set up such a system enabling ciphered contents data to be decoded exclusively for the verified proper users.

Please re-write paragraph [0013] to read as follows:

[0013] A number of the contents data distribution systems cited above provides specific users with ciphered contents data via internet service lines or via storage in a recording medium such as a DVD or a CD by way of delivering a specific contents key for decoding ciphered contents data exclusively to those verified proper users. Further, such a system is also proposed, which initially ciphers such a contents data key for preventing a malfeasant from illegally duplicating contents data and then delivers the ciphered contents data key to verified proper users in order to decode the ciphered contents data key by applying such a decoding key solely reserved by the verified proper users, whereby enabling them to utilize the delivered contents data key.

Please re-write paragraph [0014] to read as follows:

[0014] Generally, such a judgment to identify whether a corresponding user is verified as the proper one or not is executed prior to distribution of ~~a~~ contents data or a contents data key between a contents data provider for transmitting the contents and a specific device on the part of an individual user. When executing such a conventional authenticating process~~,~~ initially, the identity ~~entity~~ of the opposite party is confirmed, and then, ~~such~~ a session key solely effective for the related communication is generated. Only after completing the authenticating process~~,~~ is ~~a~~ contents related data or the contents data key ~~is~~ ciphered using the thus generated session key to conduct the related communication. There are two kinds of authenticating methods: one ~~including a mutual authentication by way of~~ utilizing the above cited common key ciphering method, and the other ~~one~~ utilizing the above cited open key ciphering method. However, in the case of the authentication utilizing the common key, another common key is required to deal with an expanded system construction, thus generating inconvenience in the process for renewing the related keys. On the other hand, in the case of utilizing the open key ciphering method, the calculation load and the volume of required memory are respectively large. Accordingly, it is by no means desirable to further provide individual devices with additional processing means.

Please re-write paragraph [0015] to read as follows:

[0015] The present invention is to provide such a data processing apparatus, such a data processing method, such a license system, and such a program providing medium, which are respectively capable of properly controlling a license in the utilization of contents data via a plurality of devices under the control of a hierarchical key tree structure and yet capable of restricting utilization of contents data based on a license even when ~~in the case of~~ recording or reproducing data via ~~such~~ a memory device ~~devoid of such function to~~ which cannot execute mutual authentication by way of

distributing an authentication key for solely enabling such a properly licensed device to decode relevant data via utilization of the hierarchical key distribution tree structure without necessarily relying on the mutual authentication process executed between transmitters and receivers of data as cited above.

Please re-write paragraph [0021] to read as follows:

[0021] It is so arranged that, among a plurality of data processing apparatuses, only ~~such~~ a data processing apparatus ~~entitled~~ with a proper license is enabled to decode the enabling key block (EKB), whereas any ~~of such~~ improper data processing apparatuses devoid of a proper license are~~is~~ unable to decode the enabling key block (EKB), t~~w~~hereby preventing any ~~of such~~ improper data processing apparatus~~es~~ from illegally decoding the enabling key block (EKB)~~so that any of such improper data processing apparatuses will be revoked~~.

Please re-write paragraph [0088] to read as follows:

[0088] The personal computer 100 can be connected to a variety of network service lines such as internet service lines and public telephone circuit lines or the like. For example, it is possible for the personal computer 100 to receive a variety of data including audio data, picture data, and programs via a network service line from a host computer owned by a service provider (not shown) presenting data service via an EMD (Electronic Music Distribution), and then, to decode the received data as required before delivering the decoded data to the reproducing apparatus 25. When receiving ~~a~~ contents data, the personal computer 100 executes an authentication process and a money levying process as required with~~between~~ a host computer owned by a service provider. Further, the personal computer 100 also outputs a variety of data received via a CD or a DVD to the data reproducing apparatus 200.

Please re-write paragraph [0090] to read as follows:

[0090] As shown in FIG. 2, whenever processing for shifting data, reproducing data

such as music data and picture data, recording data and duplicating data among the above described personal computer 100, the reproducing apparatus 200, and the storage device 300, a mutual authentication process is executed among data shifting devices, ~~t~~whereby preventing data from being shifted by applying unauthorized equipment. This process will be described later on. Further, whenever distributing contents data via network service lines or a variety of recording media or shifting contents data between the above personal computer 100 and a data reproducing apparatus or between a data reproducing apparatus and a storage device such as a memory card for example, the security of the contents data can be preserved by way of ciphering the contents data.

Please re-write paragraph [0097] to read as follows:

[0097] In the system in which a variety of devices and applications are jointly existent, it is so arranged that the above devices 0, 1, 2, and 3, corresponding to the portion encircled by the dotted line shown in FIG. 3, are installed as a single group utilizing an identical recording medium. For example, after a ciphering process, a provider delivers the ciphered common contents data or such a contents data key commonly usable by individual devices to those devices encircled by the dotted line. In another example, each of the devices outputs ciphered data related to payment of charge on the use of contents data to a provider or a financial organization. On the other hand, such a related party normally receiving data from and transmitting data ~~from and~~ to individual devices, such as a provider or a financial organization designated for settling accounts, executes a process for transmitting relevant data en bloc to the devices 0, 1, 2, and 3, corresponding to the portion encircled by the dotted line shown in FIG. 3, as a single group. Actually, there are a plurality of such groups in the tree structure shown in FIG. 3. Such a related party normally receiving data from and transmitting data ~~from and~~ to individual devices, such as a contents data provider or a financial organization, functions itself as a means for distributing message data.

Please re-write paragraph [0104] to read as follows:

[0104] The devices K0000 and K0001 further decode the ciphering key Enc (K(t) 0, ~~and~~ K(t) 0) corresponding to the second rank shown in A of FIG. 4, ~~t~~whereby respectively acquiring the updated node key K(t) 0. The devices K0000 and K0001 further decode the ciphering key Enc (K(t) 0, ~~and~~ K(t) R) corresponding to the uppermost rank shown in A of FIG. 4, ~~t~~whereby respectively acquiring the updated node key K(t) R. In this way, it is possible for the devices 0, 1, and 2 to individually acquire the updated node keys including K(t) 001, K(t) 00, K(t) 0, and K(t) R. The i~~I~~ndex shown in A of FIG. 4 respectively designates absolute addresses of the node keys and leaf keys usable as the decoding keys.

Please re-write paragraph [0106] to read as follows:

[0106] The enabling key block (EKB) shown in B of FIG. 4 is applicable to ~~such~~ a case in which a new contents data commonly owned by specific groups is distributed. For a concrete example, assume that those devices 0, 1, 2, and 3 of such a group encircled by the~~a~~ dotted line shown in FIG. 3 individually utilize a certain recording medium and require provision of a new contents data key K(t) con in common with each other. In this case, using a node key K(t) 00 updated from the node key K00 in common with the devices 0, 1, 2, and 3, ~~such a~~ data Enc (K(t) 00, ~~and~~ K(t) con) generated by way of ciphering an updated common contents data key K(t) con is distributed in conjunction with the enabling key block (EKB) shown in B of FIG. 4. As a result of this distribution process, such a contents data key can be distributed as ~~the~~ data that can not be decoded by those devices of other groups including the device 4.

Please re-write paragraph [0109] to read as follows:

[0109] FIG. 5 presents ~~such~~ a process executed by a device 0 which has received data Enc (K(t) 00, ~~and~~ K(t) con) ciphered from an updated common contents key K(t) con by applying K(t) 00 as an example of a process to generate a contents key K(t) con

at such a moment corresponding to "t" and also the (EKB) shown in B of FIG. 4 respectively received via a recording medium. Concretely, this exemplifies ~~such~~ a case in which message data ciphered by applying the (EKB) is converted into the contents key K(t) con.